

[print out](#)

Publication number 351034

Title Multicast transmission in a radio network

Publication Date 1999/01/21

Certification_Number 100595

Application Date 1997/09/26

Application No. 086114111

IPC H04B-007/24

Inventor RAIVISTO, TOMMIFI

Applicant NOKIA TELECOMMUNICATION OY.FI

Priority Number 1997/09/24 FI 19970003772

 1997/11/04 TH 19970040515

 1997/09/30 US19970940375

Abstract A sort of multicast transmission in a radio network, including a BTS and a number of MS, where the method including at least the following steps: paging the signal by means of at least 1 BTS, connection the mobile end to the paging message; the other steps are: formulating at least 1 paging message to a multiple paging message; transmission of the symbol of the multiple paging data to a selected mobile end (MS1, MS2, MS3), including the group at least 2 mobile terminals, and receiving and reply at the group of mobile terminals by means of the transmitted symbol for the multiple paging message.

**Patent Right
Change**

Application number	086114111
Authorization note	No
Qualification right note	No
Transfer Note	No
Inheritance Note	No
Trust note	No
Objection note	No
Exposure Note	No
Invalidation date	20030121
Withdrawal date	
Issue date of patent right	19990121
Due date of patent right	20170925
Due date of annual fee	20030120
Due year of annual fee	004

公告本

申請日期	86.9.26
案 號	86114111
類 別	1H04K/00, 1H04B/24

351034

A4
C4

351034

(以上各欄由本局填註)

發明專利說明書

一、發明 新 型 名 稱	中 文	於一無線電網路中之多重廣播傳輸
	英 文	MULTICAST TRANSMISSION IN A RADIO NETWORK
二、發明 創 作 人	姓 名	多美瑞維斯圖
	國 籍	芬蘭
	住、居所	芬蘭黑耳辛基市芬-00710 陸斯基泰 16 I 54 號
三、申請人	姓 名 (名稱)	芬蘭商·諾基亞電訊股份有限公司
	國 籍	芬蘭
	住、居所 (事務所)	芬蘭伊斯帕芬-02150 肯雅拉得太 4 號
	代 表 人 姓 名	1. 邁克安第拉 2. 伊斯克富來門

裝

訂

線

351034

(由本局填寫)

承辦人代碼：
大 類：
I P C 分類：

A6

B6

本案已向：

國(地區) 申請專利，申請日期： 案號： ，☐有 ☒無主張優先權

1. 本案已向芬蘭申請專利，申請日：1997年9月24日 案號：973772 號
2. 本案已向泰國申請專利，申請日：1997年11月4日 案號：040515 號
3. 本案已向美國申請專利，申請日：1997年9月30日 案號：08/940,375 號

有關微生物已寄存於： ，寄存日期： ，寄存號碼：

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

線

經濟部中央標準局員工消費合作社印製

四、中文發明摘要（發明之名稱：

於一無線電網路中之多重廣播傳輸

本發明有關於一用以於一無線網路中多重廣播之方法，該網路包含至少一基地台(BTS)及多數行動終端(行動台，MS)。該方法包含步驟：廣播來自至少一基地台(BTS)之廣播訊息，於諸行動終端接收該廣播訊息。本發明之特徵在於，其更包含以下步驟：公式化至少一廣播訊息成為一多重廣播訊息，傳送需要回復該多重訊息之資訊的符記至選定之第一群行動終端，該群包含至少兩行動終端，及在該群行動終端使用所傳送之符記，以允許多重訊息之接收及回復。

英文發明摘要（發明之名稱：

五、發明說明()

[發明領域]

本發明有關於一種於無線網路中，提供訊息服務給選定用戶之多重廣播服務。

[發明背景]

於數位 GSM 行動通訊系統(泛歐全球行動通訊系統)，除了語音及資料連接外，一短訊息服務也被執行。短訊息係被以網路之其他發信，沿著控制及發信頻道傳送。短訊息服務可以被分成點對點及區域廣播服務。點對點短訊息可以是行動起源或是行動中斷。區域廣播短訊息是被由基地台傳送並試著被用於所有為傳送涵蓋區域中之行動台。區域廣播服務之例子是交通及氣象資訊傳送。

附圖第 1 圖顯示一 GSM 行動通訊系統之簡化方塊圖。該行動台 MS 是經由無線路徑連接至一基地收發台 BTS，於第 1 圖中為基地台 BTS1。一基地台次系統 BSS 包含一基地台控制器 BSC 及由其所控制之基地台 BTS。一行動服務變換中心 MSC 通常控制幾個基地台控制器 BSC 並係連接至其他之行動服務變換中心及一 GMSC(開道行動服務變換中心)。經由 GMSC，該 GSM 網路係連接至其他網路，例如 PSTN(公用服務電話網路)，其他行動通訊網路 PLMN，ISDN 網路，智慧網路 IN，或短訊息服務中心 SMSC。整個 GSM 系統之操作是由操作及維持中心 OMC 所監視。

第 2 圖例示出三個區域 C1, C2, C3，其提供區域廣播

五、發明說明()

訊息給所有之定位於這些區域內之行動台 MS，諸行動台包含標示 MS1 者。也可能只傳送來自某些區域，例如來自區域 C1 及 C2 之區域廣播訊息。區域廣播訊息係由一區域廣播實體 CBE，例如，一新聞通訊社所創造，並經由一適當行動通訊網路傳送至行動台 MS。於此例中，該 CBE 傳送區域廣播訊息至一連接至 GSM 網路中之基地台控制器(BSC)之區域廣播中心 CBC。該區域廣播中心 CBC 控制在個別 BTS 上之區域廣播頻道上之訊息傳輸，並經由 BSC 傳送訊息至每一被定址之 BTS 上。該區域廣播係被傳送通過於 BTS 之區域廣播頻道(BCCH)中或於呼叫頻道(PCH)中之空中界面。區域廣播係試著去用於所有接收行動台，因此，它並不需要定址或加密。對於區域廣播之一更詳細之說明，請參考 GSM 規格書 GSM 03.41 “歐洲數位蜂巢式通訊系統(階段 2)；短訊息服務區域廣播之技術了解(SMSCB)”。

為了實現點對點之短訊息服務，該 GSM 網路係連接至短訊息服務中心 SMSC。該 SMSC 藉由傳送於 GSM 網路外之短訊息至一行動用戶，及由一行動用戶傳送至另一用戶或其他在 GSM 網路外可以接收短訊息之單元，而形成於一特定短訊息網路及 GSM 網路間之連接。一行動終端短訊息係由短訊息網路，經由短訊息服務中心 SMSC 發送至 GSM 網路之 MSC 並經由適當之 BSC 及 BTS 傳送至行動台 MS，即，於第 1 及 2 圖中經由 BTS1 至 MS1。因此，一行動啓始短訊息為了能夠被傳送至適當之短訊息網路，由

五、發明說明 ()

MS 經由 BTS 及 BSC 發射至 MSC，其然後由 GSM 網路傳送短訊息至 SMSC。短訊息係被透通地傳送於短訊息服務中心 SMSC 及行動台 MS 間之網路中。

通訊之機密性係有時候例如被安排以加密。第 3 圖示出一已知可以被用以保護通訊之對稱加密演譯法之方塊圖。該對稱加密演譯法係基於由通訊諸方所共用之秘密鑰。於 A 方，要被送至 B 方之訊息 M 於第 3 圖中之方塊 E 中被以共用秘密鑰 K 加密。該訊息係被傳送於一傳送路徑上，成為加密密碼文 C，其係可以為示於第 3 圖中之方塊 D 中，以相同之秘密鑰 K 所解密。經由解密方 B 取得原始訊息資訊 M。一偷聽傳送之入侵者需要知道秘密鑰 K，以讀取及了解所傳送之加密文 C。該對稱演譯法之加密及解密可以表示為公式：

$$C = E_K(M)$$

$$M = D_K(C),$$

其中，C 是加密文，M 是一般文， E_K 是具有秘密鑰 K 之加密，及 D_K 是具有秘密鑰 K 之解密。現行加密並不經由 GSM 網路，而施加至短訊息，除了於空中界面外。

已知短訊息服務之問題為訊息不是被傳送至所有傳送涵蓋範圍中之行動台(區域廣播)，就是以指定傳送方式一次只給一定址行動台(點對點)。對於傳送訊息至一選定群之行動台，該兩傳送方法均不是有用，因為先前技藝之區域廣播不能直接指向某些行動台，及用以傳送具有幾個點對點短訊息之相同訊息至一群行動台，造成於網路中太

五、發明說明()

多之發信並需要相當長之時間，以提供訊息給所有之接收者。

[發明概要]

本發明之目的是提供一多重廣播傳輸至一選定群行動台，並以一減少於網路中之發信之方式進行。

這是藉由使用依據本發明之方法加以完成，該方法特徵於如同申請專利範圍第1項所述者。本發明之特殊實施例係呈現於附屬項中。

本發明關係於一於獨立項第11項中所述之特徵之佈置。本發明之特殊實施例是呈現於附屬項第12項中。

本發明係基於一廣播訊息係被用於多重廣播傳送且於一行動終端需要一符記，以回復被送於用以多重廣播之廣播訊息中之資訊。該符記係被例如以點對點短訊息，傳送至選定行動終端。於本案之主要實施例中，用以多重廣播之區域廣播訊息係被加密，及用以解密之鑰係只被傳送給被賦與接收多重廣播訊息之行動終端。諸行動台儲存被傳送之符記，於此例為加密鑰，於其記憶體中，例如，SIM卡中。於本案之次實施例中，選定之行動終端係被致能以接收及回復多重廣播訊息。被傳送之符記是一除去限制之命令，以回復在行動終端之多重廣播傳輸。例如，該命令可以是一開始收聽廣播之指定或調至某一頻道之指定。

依據本發明之方法之優點是其提供，以訂戶為基礎，實現一短訊息服務至一選定群之行動終端之方法。

五、發明說明 ()

依據本發明之方法之另一優點是其使用很少之網路容量，因為該資訊可以以只有一短訊息被傳送至幾個行動終端。

依據本發明之優點及安排是符記傳送及多重廣播訊息之回復對於行動用戶是透通的。

[圖式之簡要說明]

本發明之較佳實施例將參考附圖加以說明，其中

第1圖示出本發明之基本之行動通訊網路之部件；

第2圖示出一先前技藝區域廣播網路；

第3圖示出一已知對稱加密演譯法之方塊圖；

第4圖示出依據本發明之主實施例之多重廣播網路；

第5圖示出依據本發明之主實施例之行動台之功能部件；

第6圖示出本發明之主實施例之流程圖；

第7圖示出依據本發明之次實施例之多重廣播網路；及

第8圖示出本發明之次實施例之流程圖。

[主要部件圖號對照說明]

BTS	基地台
MS	行動終端(行動台)
BSS	基地台次系統
BSC	基地台控制器
GMSC	開道行動服務變換中心
OMC	操作及維持中心

五、發明說明()

C 區域
CBC 區域廣播中心
CBE 區域廣播實體
SMSC 短訊息服務中心
SM 短訊息

[本案之詳細說明]

本發明係可以被應用至任何之網路中。本發明將於以下使用數位行動通訊網路系統 GSM 為例，作更詳細之說明。第 1 圖示出如先前所述之一 GSM 網路之一簡化結構。為了更詳細說明 GSM 系統之操作及結構，請參考 GSM 規格及“用於行動通訊之 GSM 系統”，M. Mouly & M. Pautet, Palaiseau, France, 1992, ISBN:2-9507190-0-7。

以下，本發明之主要實施例係藉由參考第 4，5 及 6 圖加以更詳細說明。於本案之主要實施例中，需用以多重廣播訊息回復之符記係加密鑰。該加密鑰係用以在傳送前加密該多重廣播訊息，並在選定行動台解密該多重廣播訊息。

第 4 圖示出具有區域 C1，C2 及 C3 之多重廣播之例子。於每一區域之中，基地台 BTS1，BTS2，BTS3 之一於相關之區域中，作為行動台 MS，MS1，MS2，MS3。於第 4 圖之網路中，行動用戶可以以依據本發明之多重廣播方法，來指定至一特殊服務，例如，十大新聞傳送。例如，於第 4 圖中，行動台 MS1，MS2 及 MS3 已經被一電

五、發明說明 ()

話所指定為一點對點短訊息，或例如，藉由付一訂戶費給服務公司之帳戶，而預訂其想要之特殊服務。依據本發明，該短訊息服務中心 SMSC 傳送一包含一用於該服務之加密鑰 K 點對點短訊息，給該群特殊服務用戶 MS1，MS2 及 MS3。於第 4 圖中這些被標示 SM 之點對點訊息係經由 GSM 網路被傳送至行動台，如同先前相關於先前技中所述者。為了清楚起見，該短訊息流程不被示於第 4 圖中。依據本發明之加密鑰 K 是被有利地儲存於行動台 MS1，MS2 及 MS3 之 SIM 卡中。另一方法是儲存加密鑰於行動台之其他部件中，例如，於行動設備部件中。

於第 4 圖中，該區域廣播實體 CBE 依據先前技藝啓始區域廣播訊息。依據本發明，這些用以多重廣播傳輸之區域廣播訊息，係於單元 E 中被以加密鑰 K 加密。所使用之加密演譯法可以是例如任何對稱加密演譯法。用以加密該多重廣播訊息之加密單元可以例如被定位於 CBE 中。該區域廣播中心 CBC 控制這些基地台 BTS1，BTS2，BTS3 之區域廣播，並送出區域廣播訊息至被定址之基地台。基地台廣播這些加密之區域廣播訊息。所有位於區域 C1，C2，C3 區域內之行動台接收該加密區域廣播訊息，但只有預定該特殊服務之行動台可以解密並讀取該訊息。

第 5 圖示出依據本發明之一基地台 MS1 之主實施例。其他實現本案之方法之主實施例之行動台 MS2，MS3 之功能是類似於 MS1。依據本發明，MS1 儲存被接收於點對點短訊息中之加密鑰 K 於一用於隨後取出之 SIM 卡中。

五、發明說明()

當接收加密區域廣播訊息 C 時，MS1 識別該訊息並由記憶體，例如，位於 SIM 卡中之記憶體中，選擇正確之加密鑰 K。MS1 於方塊 D 中，以所選之鑰 K 解密該接收訊息 C，並取得原始本文形式之短訊息 M。由用戶之觀點，多重廣播訊息之鑰傳送及解密是完全透通的。

若有同一行動台 MS 預定幾個特殊服務，則需要幾個加密鑰給行動台。這些加密鑰必須被加以識別，以施加給正確之加密訊息。例如，一加密訊息可以使用訊息之訊息識別器欄位來識別。該欄位識別出訊息之來源及種類。該訊息識別器欄位是未被加密。基於該訊息識別值，行動台然後選擇相當於該訊息所代表之特殊服務之加密鑰 K。

第 6 圖示出依據本發明之主實施例之方法之流程圖。於第 6 圖中之步驟 61，用於解密之加密鑰 K 隨著點對點短訊息被傳送給選定之行動台。用於多重廣播之區域廣播訊息係以加密鑰 K 加以加密(步驟 62)。隨後，加密訊息被由定址之基地台所廣播(步驟 63)並被位於傳輸涵蓋區域內之行動台所接收。選定行動台選擇相關於該接收之加密訊息之加密鑰 K(步驟 64)並以正確鑰 K 解密該訊息(步驟 65)，在此後，訊息係可讀並以可了解之一般文形式顯示。

第 7 圖示出依據本發明之次實施例之多重廣播網路之例子。如同於上述之本案主實施例，行動台 MS1，MS2，MS3 被指示想要預定依據本發明多重廣播方法所提供之特殊服務。於本案之次實施例中，短訊息服務中心 SMSC 傳送一包含一使得行動台開始回復於多重廣播中之特殊

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

頁

五、發明說明()

服務之命令，給該群之特殊服務用戶 MS1，MS2，MS3。這命令可以包含調整傳送頻道之指令及/或一訊息作用為一種密碼，以允許行動台回復多重廣播服務。這些點對點短訊息於第 7 圖中係被標示為 SM。該多重廣播訊息被以相同於先前技藝所述之有關區域廣播訊息之方式，加以啓始，發送及廣播。

於本案之次實施例中，對於利用予以多重廣播之區域廣播訊息之限制是行動台。於傳送範圍區域中之所有行動台係可以收聽該特殊多重廣播傳送，但只有預訂該多重廣播服務之行動台 MS1，MS2，MS3 可以藉由特殊致能點對點短訊息 SM 回復該多重廣播之資訊。在第 7 圖中其他被標示 MS 之行動台並不能回復該多重廣播之資訊。

第 8 圖示出依據本發明之次實施例之方法之流程圖。於本發明之次實施例中，於多重廣播訊息中之資訊之回復係可以以一特殊命令於選定行動台完成。於第 8 圖之步驟 81 中，該 SMSC 傳送致能點對點訊息至該群選定行動台。該被定址之基地台以相同於先前技藝之區域廣播訊息之方式，來廣播該多重廣播訊息(步驟 82)。該訊息是於選定行動台被接收及回復(步驟 84)。

本案之主實施例及次實施例之符記傳送訊息可以被加密或不加密，而提供連接之保安。

於本發明之其他實施例中，相對於點對點之短訊息傳送，符記可以藉由郵寄或例如以鍵盤經人工操作而傳送至選定之行動台。所傳送之符記，例如用以加密區域廣播訊

五、發明說明()

息之加密鑰 K 可以被定期地改變，以例如為了保全及送發票之目的。新符記係被傳送給作動之用戶，即給例如已經付費之用戶。當舊符記已經過期時，新的符記被傳送。新符記係需要以用於多重廣播訊息之回復。本發明外之其他實施例係相當於上述之主及次實施例所述者。

圖式及相關說明係只是用於說明本案之原理。本案之方法可以在申請專利範圍中加以改變。本案並不侷限於例示之 GSM 網路中，同時，也可以應用於任何之無線網路中。因此，行動台之例子應可以了解是任何無線網路中之行動終端。雖然本案以關於 GSM 網路中之區域廣播訊息加以說明，但本案可以被用於所有位於該區域中之行動終端，例如於 GPRS(一般分封無線服務)中之點對多點訊息。本案之主實施例之功能也可用於不是上述之對稱演譯法外之加密演譯法中。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

六、申請專利範圍

- 1.一種用以於無線網路中多重廣播之方法，該網路包含至少一基地台(BTS)及多數行動終端(MS)；其中，該方法至少包含下列步驟：

由至少一基地台(BTS)廣播廣播用訊息；

於行動終端接收該廣播訊息；

其特徵在於該方法更包含步驟：

公式化至少一廣播訊息成為一多重廣播訊息；

傳送一需用以回復該多重廣播之資訊之符記至一選定第一群行動終端(MS1, MS2, MS3)上，該群至少包含兩行動終端，及

於該群行動終端使用該被傳送之符記，以允許多重廣播訊息之接收及回復。

- 2.如申請專利範圍第1項所述之方法，其中，該方法包含步驟：

傳送一加密鑰(K)至一選定群之行動終端(MS1, MS2, MS3)，該群包含至少兩行動終端；

以該加密鑰(K)加密一廣播訊息，在廣播該訊息之前；

在該選定群行動終端(MS1, MS2, MS3)，以該被傳送之加密鑰(K)解密該廣播訊息。

- 3.如申請專利範圍第2項所述之方法，其中，該方法更包含步驟：

以點對點短訊息(SM)，傳送該加密鑰(K)至該群行動

六、申請專利範圍

終端 (MS1, MS2, MS3)。

- 4.如申請專利範圍第2或3項所述之方法，其中，該方法更包含步驟：

於行動終端，儲存一加密鑰(K)。

- 5.如申請專利範圍第2或3項所述之方法，其中，該方法更包含步驟：

於該行動終端之SIM卡上，儲存該加密鑰(K)。

- 6.如申請專利範圍第2項所述之方法，其中，該方法更包含步驟：

改變該加密鑰(K)；及

傳送新加密鑰至一選定之第二群行動終端上。

- 7.如申請專利範圍第6項所述之方法，其中，該選定第二群行動終端不同於該選定第一群行動終端。

- 8.如申請專利範圍第1, 2或3項所述之方法，其中，該方法更包含步驟：

由附著至該訊息之訊息識別器，來識別該多重廣播訊息；及

基於該多重廣播訊息之訊息識別器，來選擇相關該訊息之加密鑰(K)。

六、申請專利範圍

9.如申請專利範圍第1項所述之方法，其中，該方法包含步驟：

傳送一致能命令，給一選定群行動終端(MS1，MS2，MS3)，該群包含至少兩行動終端；及

於該等已接收致能命令之行動終端，致能該多重廣播訊息之接收及回復，

10.如申請專利範圍第9項所述之方法，其中，該方法包含步驟：

傳送具有點對點訊息(SM)之致能命令至該群行動終端(MS1，MS2，MS3)。

11.如申請專利範圍第9或10項所述之方法，其中，該方法包含步驟：

藉由調諧行動終端至正確頻道，而於該群行動終端，致能該多重廣播訊息之接收及回復。

12.一種用以於無線網路中多重廣播之配置，其包含：

一訊息源(CBE)，用以產生廣播訊息；

一廣播中心(CBC)，用以控制廣播訊息之廣播；

諸基地台(BTS1，BTS2，BTS3)，其廣播該廣播訊息；

行動終端(MS)，其接收該廣播訊息；

其特徵在於，該配置更包含：

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

一傳送單元(SMSC)，用以傳送一符記至一些行動終端；

一致能單元(D)，用以在該行動終端，致能該多重廣播訊息之接收及回復。

13.如申請專利範圍第12項所述之配置，其中，該配置包含：

一傳送單元(SMSC)，用以傳送一加密鑰(K)至一些行動終端；

✓ 一儲存單元(SIM)，用以儲存該被傳送之加密鑰(K)於行動終端上；及

一加密單元(E)，用以加密該用以多重廣播之廣播訊息；及

一解密單元(D)，用以於行動終端，解密該被加密之廣播訊息。

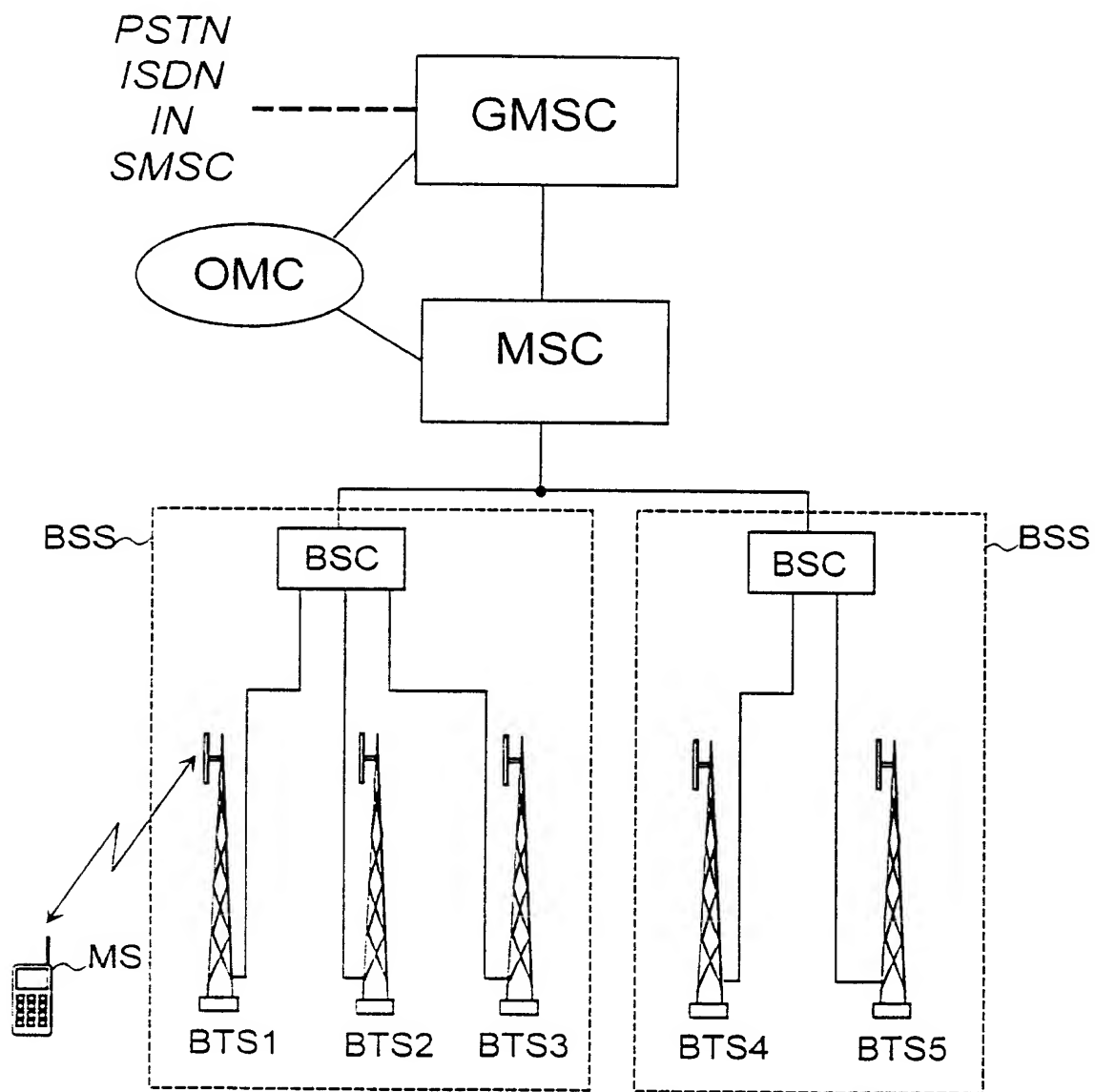
14.如申請專利範圍第12或13項所述之配置，其中，該廣播訊息是區域廣播訊息。

(請先閱讀背面之注意事項再填寫本頁)

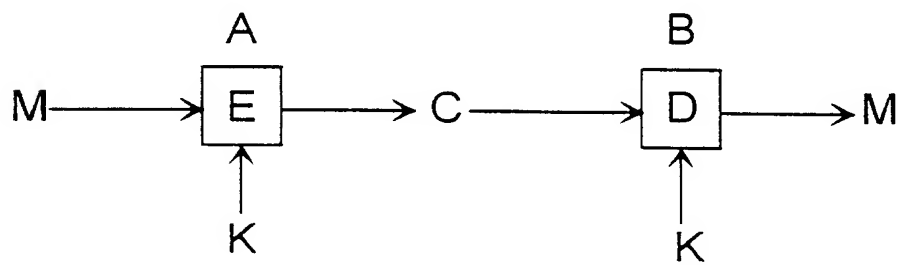
裝

訂

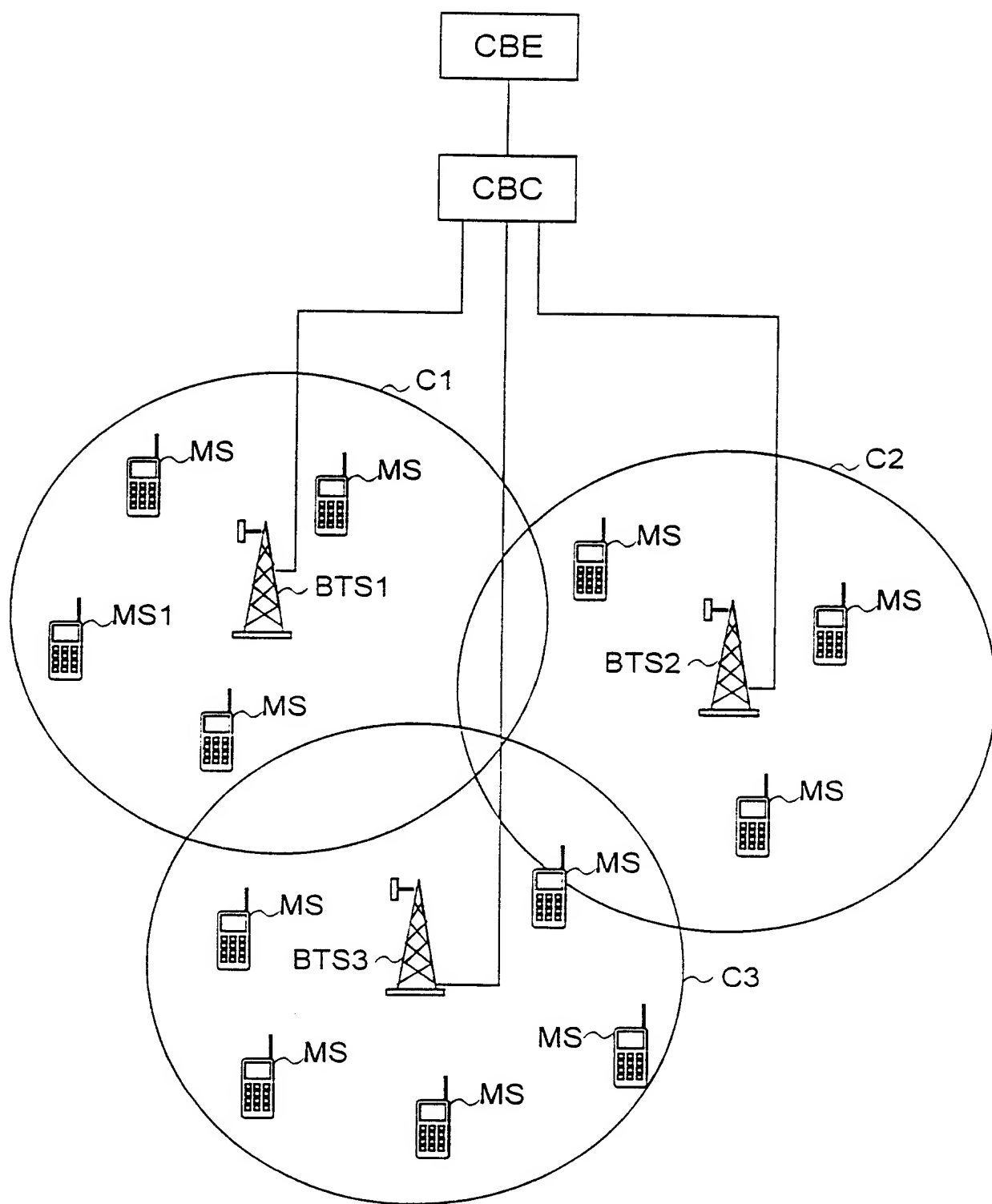
原



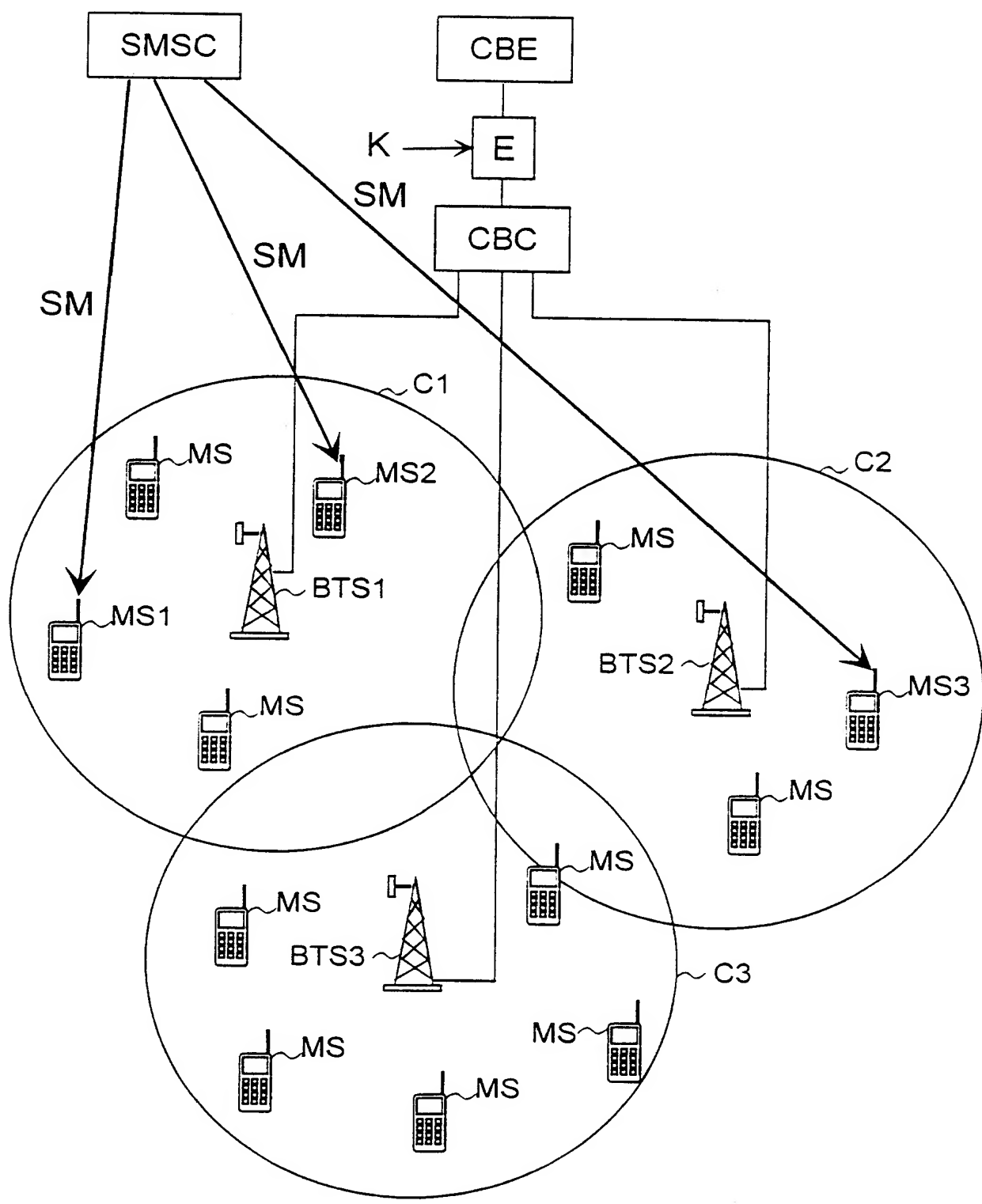
第 1 圖



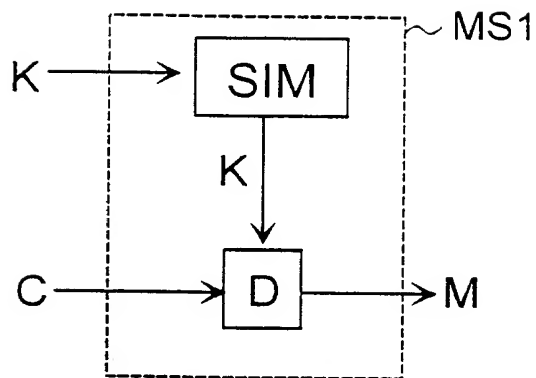
第 3 圖



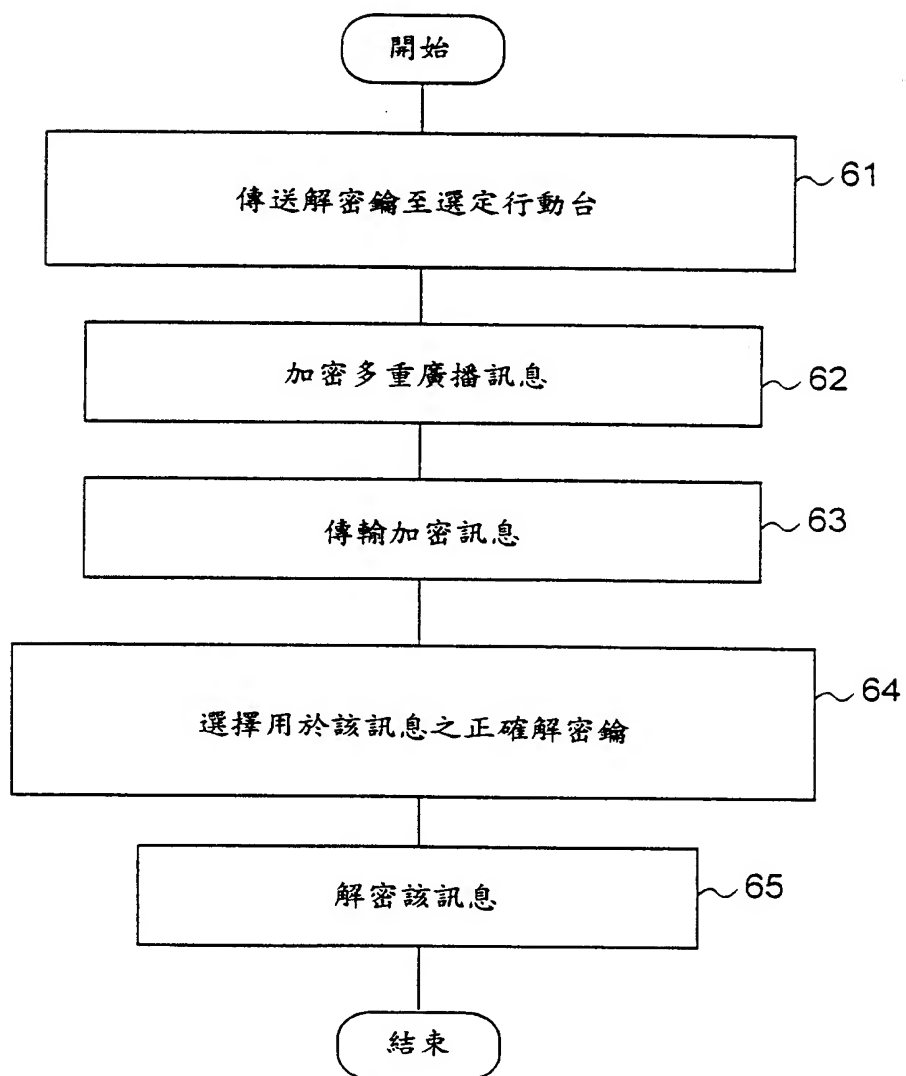
第 2 圖



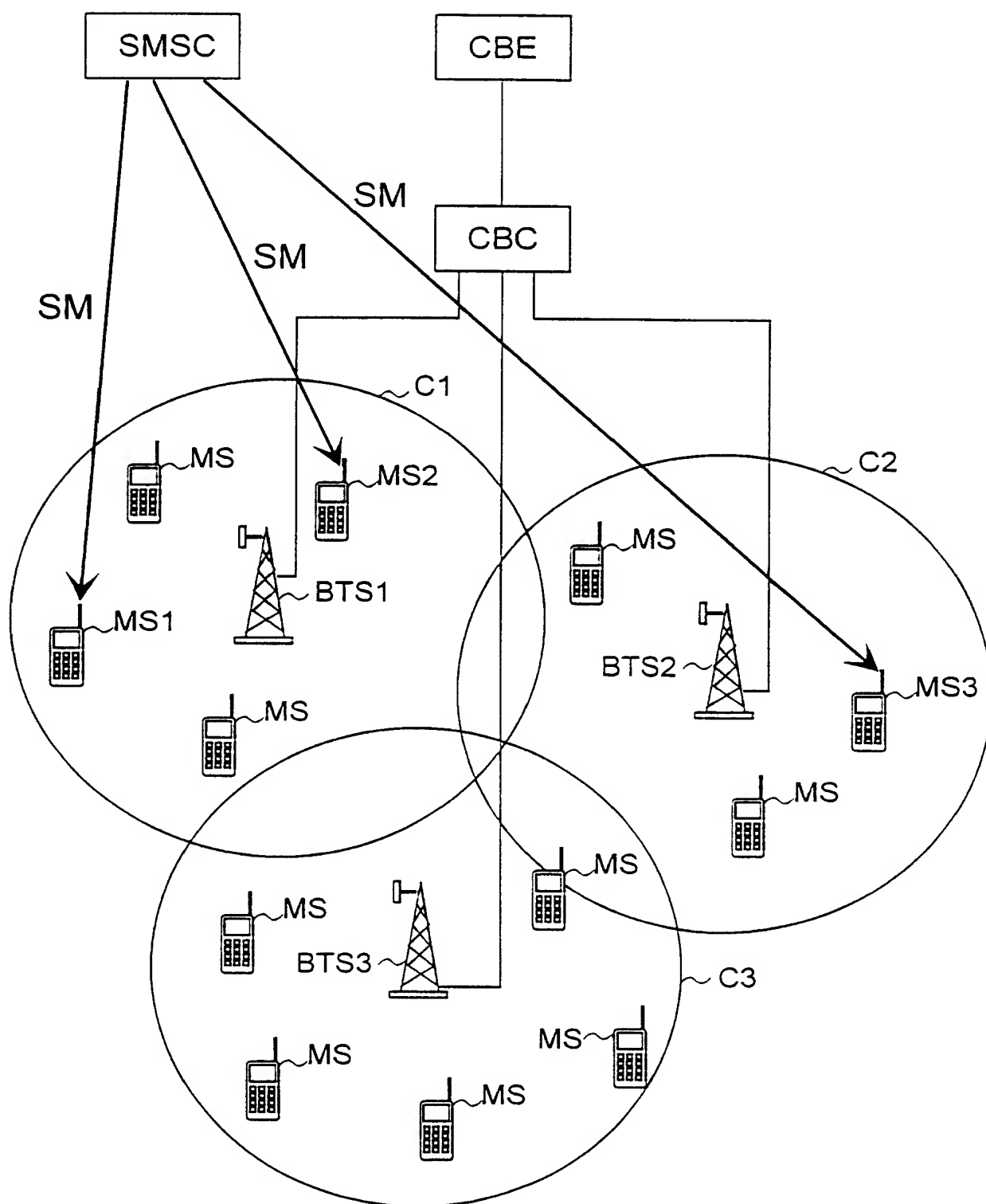
第 4 圖



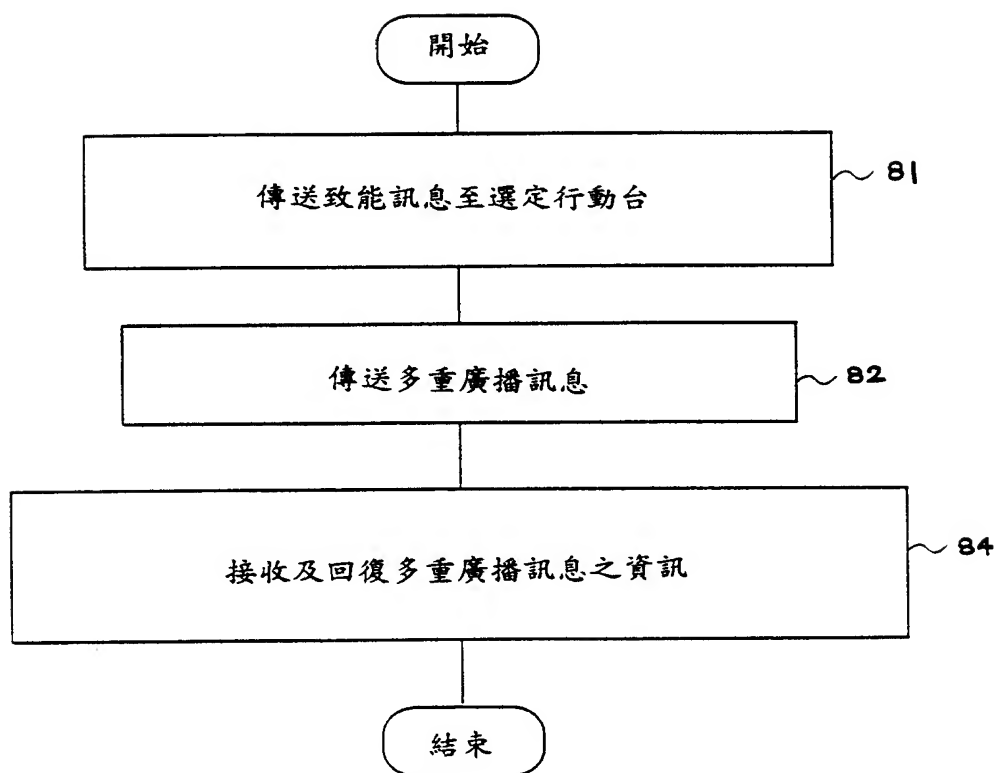
第 5 圖



第 6 圖



第 7 圖



第 8 圖